Baarnsche Dijk 4 D
3741 LR Baarn
www.edsn.nl
T (035) 54 80 180
F (035) 54 80 184

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC023 Beveiligde verbindingen

Status	Vastgesteld		
Versienummer	1.0	**Versiedatum**	27 april 2013
Documentnaam	TC023 Beveiligde verbindingen		

Behandeld door de Technische Commissie			
	IC Klant	**IC Wholesale–E**	**IC Wholesale-G**
Datum akkoord	**7 februari 2013**	**15 februari 2013**	**8 maart 2013**

Raakt aan	**Kleinverbruik**	**Grootverbruik**	**Wholesale**
Elektriciteit	**X**	**X**	**X**
Gas	**X**	**X**	**X**

Impact op keten	**Ja/Nee**
Codewijziging	**Nee**
Berichten	**Nee**
Ketenprocessen	**Nee**

Mogelijke impact marktrollen en EDSN	**Ja/Nee**
LV	**Ja**
PV	**Ja**
MV	**Ja**
RNB	**Ja**
LNB	**Ja**
EDSN	**Ja**

Vastgesteld door NEDU op 24 april 2013
Invoering in markt uiterlijk per 1 juli 2014

Contact	
Technische Commissie	TC@edsn.nl

Management samenvatting

De sector wisselt al ruim 10 jaar gegevens uit in de ketenprocessen middels beveiligde internetverbindingen. De eisen aan deze beveiliging schreiden voort. De sector heeft eerder gekozen om met de beveiliging van het berichtenverkeer de richtlijnen van de overheid te volgen (PKI-overheid, bewaakt door Logius) De overheid past de eisen regelmatig aan, zoals de overgang op verbeterde (SHA2) beveiligingscertificaten. Het is zo langzamerhand niet verantwoord meer om in de sector verouderde versies van het beveiligingsprotocol op de verbindingen te gebruiken. Daarom wordt voorgesteld om over te gaan op een modernere versie voor de beveiliging van het verbindingen, zulks in lijn met de eisen die de overheid stelt aan dergelijke verbindingen. De invoering zou gelijk kunnen vallen met de invoering van de SHA2 beveiligingscertificaten.

Situatieschets:

De internetverbindingen (http), die tussen partijen in de sector worden opgezet voor uitwisseling van het berichtenverkeer, worden beveiligd middels encryptie protocollen. Daarmee wordt de overgezonden informatie op de transport laag beveiligd tegen ongeoorloofd meelezen. Voor de encryptie worden beveiligingscertificaten gebruikt.
Traditioneel wordt hier het Secure Sockets Layer (SSL) encryptieprotocol in de beveiliging van de communicatie over internet gebruikt. Als opvolger van SSL is een verbeterd protocol Transport Layer Protocol (TLS) ontstaan. Van zowel SSL als TLS zijn in de loop der jaren nieuwere versies vastgesteld. Communicatiesoftware van software leveranciers ondersteunt vaak meerdere, ook oudere versies van deze protocollen. Marktpartijen maken hun eigen keuze in software pakketten en leveranciers. Om te voorkomen dat verbindingsproblemen ontstaan, doordat communicatiesoftware van verschillende software leveranciers niet hetzelfde SSL of TLS level ondersteunt en daardoor niet met elkaar wil ‘praten’, bevat het protocol in het opzetten van de verbinding een ‘onderhandelingsstructuur’ om met de tegenpartij een geschikt (lager) niveau overeen te komen, die beide communicatiepartners wel accepteren. Verschillende verouderde versies van SSL en TLS worden echter al langere tijd niet meer als veilig genoeg beschouwd door Security Officers. Recente versies van TLS verbieden dan ook te onderhandelen over oudere, onveilige versie van het protocol (SSL 3.0 en lager). Dit kan echter tot verbindingsproblemen leiden als niet alle partijen over de nieuwere versies van hun communicatiesoftware beschikken.

Vraag:

Kunnen we in de sector afspraken maken over het minimale beveiligingsniveau in de beveiliging van de verbinding voor het berichtenverkeer?

Overwegingen

- Veel van ons berichtenverkeer wordt alleen op transport niveau beveiligd.
- Het verdient aanbeveling zo weinig mogelijk nog SHA1 beveiligingscertificaten te gebruiken. Het advies om over te gaan op SHA2 beveiligingscertificaten is al eerder gegeven, echter de invoering daarvan wordt na de invoering van het nieuwe marktmodel gepland.
- Gebruik maken van de nieuwste versies van de beveiligingsprotocollen geeft de grootste garantie op goede bescherming.
- TLS en SSL zijn niet helemaal gelijkwaardig, maar ook SSL wordt regelmatig geüpgrade.
- TLS kan transparant met SSL gebruikt worden, waardoor partijen de mogelijkheid hebben al eerder te migreren naar TLS.
- TLS v1.2 vereist de veiliger SHA2 beveiligingscertificaten.
- De standaard communicatiesoftware pakketten ondersteunen TLS (en SSL) al enige jaren.
- Uitvraag bij de leden van de TC leert dat deze partijen of al TLS gebruiken of verregaande plannen hebben hierop over te stappen.
- Voor de beveiliging van onze B2B verbindingen volgen wij de richtlijnen van de overheid en maken we gebruik van de PKI-overheid voor de beveiligingscertificaten.
- De overheid beveelt aan (Koppelvlak WUS, 19 oktober 2011) geen (onveiliger) SSL verbindingen meer te laten gebruiken, maar in plaats daarvan over te gaan op TLS:
    - Authenticatie op transport niveau gebeurt op basis van TLS v1.0 met tweezijdige authenticatie.
    - Client and Server authenticatie is vereist, gebruikmakend van HTTPS and TLS 1.0 [RFC 2246].
    - De TLS implementatie mag niet op SSL (v3 of lager) terug kunnen vallen.

Als voorbeeld kan worden genoemd dat het Klick (voor uitwisseling kaartmateriaal) per 1 januari 2014 over gaat op TLS (met SHA2 certificaten).

Oplossing:

De overheidsrichtlijn volgen en over gaan op TLS 1.0 of hoger, waarbij terugval op SSL v3 of lager is verboden, en deze te gebruiken met een SHA2 beveiligingscertificaat.

Impact:

Partijen besteden met regelmaat aandacht aan de upgrade van hun verbindingsprotocol. Daarmee hoeft deze upgrade geen extra belasting te zijn.

Invoeringsstrategie:

Elke partij wordt gevraagd TLS zo snel mogelijk in te voeren (vooralsnog zonder blokkade op terugval naar SSL).
Elke partij wordt geacht uiterlijk per 1 juli 2014 TLS te hebben ingevoerd. Per die datum wordt de blokkade op de terugval naar SSL sectorbreed ingevoerd.
Aanvullend geldt dat de landelijke netbeheerders een inspanningsverplichting hebben om ervoor te zorgen dat ook de buitenlandse partijen zich gaan conformeren aan dit beveiligingsniveau.

Te vervallen issues:

Geen

Versieoverzicht:

0.1 eerste aanzet door Gerrit Fokkema na bespreking in TC overleg op 16 maart 2012;
0.2 update met overheidsrichtlijn en dienovereenkomstig voorstel als besproken in TC overleg op 9 november 2012;
0.3 update na reactie TC leden vóór de vergadering van 14 december 20121;
0.4 update na bespreking in de TC vergadering van 14 december 2012;
0.5 update na conference-call TC op 25 januari 2012;
0.6 update na review door IC-Klant op 7 februari 2013;
0.7 Update na review door IC-WE en IC-WG en bespreking in de TC vergadering van 14 maart 2013.
1.0 Na vaststelling in de AV NEDU van 24 april 2013, met daar besloten toevoeging inspanningsverplichting LNB's